ment electronically. Other witnesses may have associated with them various credibility ratings. A witness may also sign as to observing the signature in either the physical presence or by watching the signature in real time in an online fashion. The witness may also be recorded using the camera or video camera on the CT/MD. As an example, the video camera on the CT/MD may record or stream the signing event to another CT/MD or server. The other CT/MD or server may store the signing event for future playback, auditing, or other purposes. Alternatively, the camera on the CT/MD may take snapshots while the signature event is taking place. An audio recorder integrated into the CT/MD may record sounds that are taking place at this time. The CT/MD may further record the GPS location of the signature event. The signature and associated meta-data related to the event may be archived to the signature document and stored locally on the CT/MD or on the server.

The collaboration event may further be enabled to record negotiation and requests by one or more parties. The collaboration product **1210** may be marked as pending or as a final version. Parties may state by selecting a touch box, an accept button, or other marker to indicate agreement.

The parties privy to the collaboration event may be required to agree to the event at a specified time, in real time or simultaneously.

The server may compare the signatures, signature images, signature strokes, time to sign, signature movement across the touch screen, to stored samples located on the device or a server. The CT/MD or server may perform handwriting recognition using a software program.

There may exist a plurality of servers enabled to stored one or more samples of the data. A server may function as an escrow server whereby the server holds authentication information or collaboration information for a specified time or rule.

The authentication system may require a plurality of authentication methods simultaneously, sequentially, temporally spaced, or geographically spaced using GPS information. One authentication method may require a voice reading while a second authentication method may require a password being entered on the device. A server may require authentication to a service by requiring a user to enter a password on the CT/MD and a code delivered by the server to the CT/MD. The server may also require authentication by requiring a user to enter a password on the CT/MD and then a password obtained from the CT/MD while the password is entered. An image may compared against a stored sample on the device or on the server. The image may also include a retinal scan that is compared against a stored sample.

The server or CT/MD may also require and obtain GPS location information for the phone during an authentication event. The server may correlate a plurality of authentication information to determine whether the collaborator is in proximity to another collaborator. The server may use an IP address to determine location. The server may also store and correlate IP addresses for authentication purposes.

FIG. **7** illustrates a CT/MD **1300** with multiple keyboards **1301**, **1302**, **1303**, **1304**, **1305**, **1306**, **1307**, **1308** spaced at different positions on a touch screen display. A user may define the ideal spacing in a configuration file. Alternatively the CT/MD or server may contain ideal spacing information. An individual's hand size and finger size may be used to create an ideal spacing of the keyboard. The finger size may be measured during a calibration process where the user places their fingers on the touch screen and the CT/MD determines the points of contact. Alternatively, a user may describe their hand type such as small, medium, or large and the system may use the associated keyboard spacing. The CT/MD may also download various keyboard spacing from a server. This spacing allows for greater vertical separation between the rows of a keypad. A horizontal separation may also be enabled or different combinations of split keyboards groups of keys, or specific keys may be configured. Keyboards **1302** and **1308** feature greater horizontal and vertical separation than a full numeric keypad organized as a row. Similarly macros or icons can be split across different areas. The location of the keyboards may be configurable by a user. The keyboards may allow for easy access to keys to prevent inadvertent selection of the wrong character. A first keyboard such as the numeric keyboard **1302** may be located at the top of the display and may appear or disappear based on the application the CT/MD. The application **1309** as shown is a spreadsheet application where character entry and numeric entry may both be required by a user.

The keys in the keyboard typically could be LCDs for displaying the respective legends, and desirably are touch sensitive.

The foregoing descriptions of specific embodiments of the present disclosure have been presented for purposes of illustration and description. They are not intended to be exhaustive or to limit the disclosure to the precise forms disclosed, and it should be understood that many modifications and variations are possible in light of the above teaching. The embodiments were chosen and described in order to best explain the principles of the present disclosure and its practical application, to thereby enable others skilled in the art to best utilize the present disclosure and various embodiments, with various modifications, as are suited to the particular use contemplated. It is intended that the scope of the disclosure be defined by the Claims appended hereto and their equivalents.

What is claimed is:

1. A system for authentication to a multifunction device based on a gesture, comprising:

the device comprising a keyboard, a processor, a camera, and a wireless transmit and receive function, and audio and video functions,

the device configured with a first authentication requirement for access to the device and a second authentication requirement for authentication to one or more applications on the device,

wherein authentication to an application requires a response to a series of authentication steps,

wherein authentication to the device or application is enabled using a gesture, wherein said gesture is a visual movement in the form of a pre-defined shape by a user,

wherein an application on the device displays an authentication request,

wherein the device displays a photo from a set of photos in the device,

wherein the device presents a question to a user on the display related to the photo,

wherein the system comprises a multi-level authentication system which includes granting access to the device and the one or more applications based on a high or low security level settings, and

wherein a key is expanded based on actuating, and ambient light detected by a light sensor on the device to facilitate easier viewing of the key.

2. The system of claim **1**, wherein the question displayed is whether the user took a photo or received a photo.

3. The system of claim **1**, wherein the authentication request requires server authentication, device authentication, and an application authentication to gain access to the device.